IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	Case No. 1:20-CR-143
	)	
v.	)	Honorable T.S. Ellis, III
	)	
ZACKARY ELLIS SANDERS,	)	Hearing: September 11, 2020
	)	
Defendant.	)	**FILED UNDER SEAL**
	)	

GOVERNMENT'S OMNIBUS RESPONSE IN OPPOSITION TO DEFENDANT'S MOTIONS TO SUPPRESS

The United States of America, by and through its attorneys, G. Zachary Terwilliger, United States Attorney for the Eastern District of Virginia, William G. Clayman, Special Assistant United States Attorney (LT), and Jay V. Prabhu, Assistant United States Attorney, files this omnibus response in opposition to the defendant's four motions to suppress. Dkt. Nos. 81, 83, 85, & 90. For the reasons stated below, the defendant's motions should be denied.

INTRODUCTION

[redacted], which led investigators to believe and Magistrate Judge John F. Anderson to conclude that there was a fair probability that child-pornography-related evidence would be found at the residence. Accordingly, Magistrate Judge Anderson issued a warrant to search the premises.

Despite the defendant's speculation, the tip was reliable and the search of his home uncovered substantial evidence that he engaged in online child-exploitation conduct on Tor and with minors he met through other means. Faced with this evidence, the defendant now attacks the warrant in four separate motions and asks the Court to grant the extraordinary remedy of excluding all evidence and statements obtained during the search of his home. But all the defendant's arguments fail. As discussed below, the warrant provided ample probable cause to believe there was a fair probability that someone in his home took multiple steps to intentionally access child pornography on Tor and that evidence of the crime would be located in the home. His arguments to the contrary are based on nothing more than a misreading of the tip and a misapplication of the relevant law on probable cause and staleness.

Similarly, the defendant has not made the proper substantial showing of misconduct or recklessness required to obtain a *Franks* hearing. Instead, he has recycled the same failed, speculative arguments regarding two portions of the tip that he relied on in his motion to compel and raised disagreements with the warrant's accurate descriptions of Tor and various other topics that do not meet the heavy burden required to obtain such a hearing. In other words, and contrary to the defendant's current arguments, the warrant was supported by probable cause and was not stale at the time the magistrate judge issued it. And even if he could identify a deficiency in the warrant—which he cannot—law enforcement plainly relied on it in good faith. Indeed, the investigation confirmed the FBI's reasonable belief that evidence of online child-pornography activity would be found at the home; the execution of the valid warrant led to significant evidence of crimes against children and the defendant's use of Tor to access child sexual abuse material. The defendant's four motions should therefore be denied.

BACKGROUND

The charges in this case stem from [redacted]. As explained below, this information led the FBI to the defendant's home in McLean, Virginia, where the FBI uncovered substantial evidence showing that he engaged in a range of child-exploitation-related activity with multiple minors.

I. Background on the Tor Network and the Target Website

The Court explained in detail how the Tor network operates in its memorandum opinion denying the defendant's motion to compel. *See* Dkt. No. 73 at 2–3. In short, and as also explained in the affidavit in support of the search warrant ("Affidavit"), Tor is an online computer network that seeks to mask a user's identifiable IP address by bouncing the user's online communications around a network of relay computer (or "nodes") run by volunteers. *See* Search Warrant Affidavit, Dkt. No. 82, Exh. 1 ("Aff.") at ¶¶ 7–14. By downloading and installing the Tor browser on a computer, a user can access the Tor network and use the browser to visit websites on the open internet as well as Tor hidden services. *Id.* Hidden services are sites that are only accessible via Tor and that have unique technical features aimed at concealing the location of the computer server hosting the website. *Id*. at ¶ 13. Unlike an open internet website address (www.justice.gov, for example), the web addresses for hidden services consist of a series of either 16 or 56 algorithm-generated characters followed by the suffix ".onion." *Id.* at ¶ 14. While these hidden services provide a powerful tool for those who wish to share information in places where the open exchange of ideas might be stifled, the anonymity provided by the network has a downside: hidden services provide a haven for criminal activity in general and the online sexual exploitation of children in particular. *See Over 80 Percent of Dark-Web Visits Relate to Pedophilia, Study Finds*, WIRED

MAGAZINE, December 30, 2014, available at: http://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/ (last visited September 9, 2020).

[redacted]

[redacted]

II. [redacted] and the Identification of the Defendant's Home

As the Court knows, [redacted]. Dkt. No. 73 at 3–4. [redacted].[1] *Id.* at 4. The FBI knows [redacted]. Aff. at ¶ 25. In fact, when the warrant issued in this case, [redacted]. *Id.* at ¶ 26.

After receiving this information, the FBI determined that the Target IP was registered to Cox Communications and sent the company a subpoena requesting information about the identity of the subscriber on May 23, 2019. *Id.* at ¶ 31. Cox identified the subscriber then as the defendant's

[1] These documents are attached to the defendant's motion to suppress, Dkt. No 86, as Exhibits 1, 2, and 3.

mother and her address as the defendant's home in McLean, Virginia.[2] In January 2020, the FBI conducted a search of public records, which showed that the defendant and his parents lived at that address. *Id.* at ¶ 34. Additionally, in February 2020, the FBI confirmed that they were still receiving mail there. *Id.* at ¶ 35.

III. The Search Warrant and the Search of the Defendant's Home

Equipped with information that [redacted], the FBI took the next natural step in its investigation and asked a neutral magistrate judge for a warrant to search the defendant's home for evidence. Specifically, FBI Special Agent ("SA") Christopher Ford prepared an Affidavit, which contained significant amounts of information, including:

- Information about SA Ford's background and experience with investigations involving the sexual exploitation of children (Aff. at ¶ 1);
- A description of the place to be searched (*id.* at ¶ 2, Attachment A);
- Background on Tor and hidden services, and the fact that hidden services are not indexed to the same degree as open internet websites by online search engines like Google (*id.* at ¶¶ 7–14, 27);
- [redacted] (*id.* at ¶¶ 15–21, 24);
- [redacted] (*id.* at ¶¶ 22–26);
- An explanation of how a Tor user could access a hidden service like the Target Website and the fact that [redacted] (*id.* at ¶¶ 27–30);

[2] Cox Communications' response is attached as Exhibit 1 to this filing.

- An explanation of the nexus between the criminal conduct and the placed to be searched—including the connection between the Target IP and the defendant's home, information about who resided at the home, and the fact that [redacted] (*id.* at ¶¶ 31–35);

- [redacted] and SA Ford's training and experience that those who have an interest in viewing child pornography often collect such content, store it in a safe and secure place in their home, and retain it for long periods of time (*id.* at ¶¶ 37–46);

- Information about how individuals who view child pornography often use computers and other electronic devices to do so, and the process and challenges of recovering information and evidence related to such activity—including evidence that an individual may have tried to delete—from such devices (*id.* at ¶¶ 36, 42, 47 – 51); and

- The items to be seized (*id.*, Attachment B).

After reviewing this information, Magistrate Judge Anderson determined that the Affidavit set forth probable cause to search the defendant's home and issued a federal search warrant. Law enforcement executed the warrant on February 12, 2020. The defendant, then 24 years old, and his parents were present in the home at the time. The defendant voluntarily agreed to be interviewed in his home and admitted to accessing child sexual exploitation material on Tor.

ARGUMENT

Before the Court are the defendant's four separate motions to suppress, totaling close to 100 pages of briefing and well over 100 pages in exhibits, in which he argues that the Affidavit lacked probable cause and asserts that he has satisfied the heavy burden required for a *Franks* on multiple portions of the Affidavit. For the reasons that follow, all four motions should be denied.

I. The Defendant's First Motion to Suppress Should Be Denied

In his first motion, the defendant relies on a misreading of the tip and his own dissatisfaction with the FBI's investigation to argue that the Affidavit lacked probable cause to believe that a crime had been committed and that evidence would be found at his home, and that

all evidence obtained from his home should therefore be suppressed. Dkt. Nos. 81 & 82. These arguments are meritless and this motion should be denied.

A. The Affidavit articulates probable cause for the search

The Affidavit provided ample probable cause to search the defendant's home. Probable cause exists when, "given the totality of the circumstances, there is a 'fair probability that contraband or evidence of a crime will be found in a particular place.'" *United States v. Richardson*, 607 F.3d 357, 369 (4th Cir. 2010) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)). It "is therefore not a high bar." *United States v. Bosyk*, 933 F.3d 319, 325 (4th Cir. 2019) (internal quotation marks omitted). Further, once such a "fair probability" exists, speculation about potential innocent explanations cannot invalidate probable cause. *See District of Columbia v. Wesby*, 138 S.Ct. 577, 588 (2018) (reversing where court "mistakenly believed that it could dismiss outright any circumstances that were 'susceptible of innocent explanation'"). Thus, a reviewing court "must accord 'great deference' to a magistrate's assessment of the facts presented to him." *United States v. Montieth*, 662 F.3d 660, 664 (4th Cir. 2011) (quoting *United States v. Blackwood*, 913 F.2d 139, 142 (4th Cir. 1990)). A review of a magistrate judge's probable cause determination is therefore limited to whether the judge had a "substantial basis for determining the existence of probable cause." *Montieth*, 662 F.3d at 664 (quoting *Gates*, 462 U.S. at 239).

Applying these principles here, the magistrate judge had a substantial basis to find probable cause to search the defendant's home. The Affidavit explains that [redacted]. Aff. at ¶¶ 22–26. [redacted]

[redacted]. *Id.* at ¶¶ 7–21, 27–29. [redacted]. *Id.* at ¶¶ 31–35. And it concludes by describing the tendency of individuals interested in viewing child pornography to store it in their homes and view it on electronic devices and how evidence of such activity, including old or deleted activity, can be recovered from such devices. *Id.* at ¶¶ 37–51. As the law requires, the Affidavit linked criminal activity—at a minimum, accessing or attempting to access the Target Website with the intent to view child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B)—to the place to be searched, and provided the neutral magistrate judge with a reasonable basis to conclude that there was a "fair probability" that contraband would be found there.

Courts across the country agree that probable cause exists to search a home when an IP address linked to that home was used to engage in online child exploitation conduct. *See United States v. Contreras*, 905 F.3d 853, 858 (5th Cir. 2018) ("[O]ur court, as well as others across the country, has found probable cause to search a residence based on just one or two uploads of child pornography [from the home's IP address]."). [3] Courts also recognize that the unique

[3] *See also United States v. Gillman*, 432 F. App'x 513, 514–15 (6th Cir. 2011) (finding probable cause to search based on user of IP address possessing and sharing one video of child pornography); *United States v. Vosburgh*, 602 F.3d 512, 526–27 (3d Cir. 2010) (finding probable cause to search based on user of an IP address's attempt to download a video purporting to be child pornography); *United States v. Richardson*, 607 F.3d 357, 361, 371 (4th Cir. 2010) (finding probable cause to search based on two emails containing child pornography from an account tied to home); *United States v. Perez*, 484 F.3d 735, 740–41 (5th Cir. 2007) (finding probable cause to search based on one-time transmission of child pornography via a webcam from an IP address).

characteristics of child pornography sites on Tor can be used to draw favorable inferences in support of probable cause based on allegations that someone at a home accessed or viewed content on such a site. *See United States v. DeFoggi*, 839 F.3d 701, 707 (8th Cir. 2016) ("Accessing [a child pornography Tor site] therefore required numerous affirmative steps by the user, making it extremely unlikely that a user would stumble upon it without knowing that its purpose was to advertise and distribute child pornography and understanding the content to be found there.").[4] Given that the Affidavit noted the difficulty of accessing the Target Website and the many steps a user would need to take to do so, it was reasonable to infer that the user of the Target IP knew what the site was and accessed it with the intent to view child pornography.

In fact, the Fourth Circuit recently found that probable cause existed to search a home when the home's IP address was used one time to visit a page on an open internet website from which a user with a password could download an encrypted child pornography file solely because a link to that page had been posted on a Tor child pornography site alongside child pornography images beforehand. *Bosyk*, 933 F.3d at 322–23, 326 (4th Cir. 2019). While there was no allegation that this user saw and clicked the link on Tor or viewed any child pornography prior to or after accessing the link, the court emphasized that it was reasonably probable that the user saw the link on Tor based on the secretive nature through which child pornography is shared online and that

[4] *See also United States v. Taylor*, 935 F.3d 1279, 1283 (11th Cir. 2019) ("You can't just Google a hidden service; rather, a user can access one of these Tor-specific sites only by knowing its exact URL address. Most Tor-site addresses comprise a random jumble of letters and numbers followed by the address '.onion'—in place, say, of '.com' or '.org'—and are shared via message-board postings on the regular internet or by word of mouth."); *United States v. Tagg*, 886 F.3d 579, 587 (6th Cir. 2018) (finding it "unlikely" that a defendant "stumbled upon [a child pornography Tor site] by accident" because, "[t]o access the site, he had to obtain the URL from someone 'on the inside' who could provide the exact sequences of numbers and letters to enter into his browser," which "creates an inference" that the defendant deliberately accessed the site); *United States v. Darby*, 190 F. Supp. 3d 520, 524–25 (E.D. Va. 2016) (same).

the user therefore likely knew the link would direct him to child pornography. *Id.* at 322, 325–28. Importantly, the court rejected the idea that the warrant needed to exclude the possibility of the user innocently accessing the link, explaining that requiring the government to rule out such speculation "demands more proof than is required to obtain a warrant." *Id.* at 327; *id.* at 329 (rejecting requirement that the warrant prove the user *must have* known the page contained child pornography in favor of proof that he *could have* known based on a fair probability).

Despite the clear link between criminal conduct and his home, the defendant has raised three general challenges to the probable cause determination here. They are all unavailing.

1. The Affidavit establishes the reliability of [redacted]

First, he argues that the Affidavit does not provide a basis to rely on [redacted] Dkt. No. 82 at 5–9. [redacted], the defendant claims that the FBI had to corroborate the tip before it would be reasonable to rely on it. *Id.* [redacted]

[redacted]. Aff. at ¶ 23, 25–26. With this as background, the FBI and Magistrate Judge Anderson had ample reason to believe that the tip was reliable. *Id.* at ¶¶ 15, 23. Accordingly, the defendant's argument that it was somehow unreasonable to infer from the Affidavit that the tip was reliable and meant what it plainly stated—[redacted]—is without merit.

2. The Affidavit supports a reasonable inference that [redacted]

Second, the defendant asserts that the Affidavit lacked probable cause because it does not provide reason to believe that someone at his home intended to view or access child pornography. Dkt. No. 82 at 10–13. Again, however, the Affidavit clearly states that [redacted]. Aff. at ¶¶ 15–21, 23, 27–29. Relying on *United States v. Falso*, 544 F.3d 110 (2d Cir. 2008), *Bosyk*, and, in a supplemental filing, *United States v. Reece*, 2017 WL 11373457 (E.D. Va. Mar. 1, 2017), the defendant claims that this is not enough. He is incorrect.

In *Falso*, 544 F.3d at 114, 121, the court invalidated a warrant because it was based on the inconclusive statement that the defendant only "appeared" to have "either gained access or attempted to gain access" to a non-Tor site associated with child pornography and because it failed to adequately describe the site as dedicated to child pornography. Here, on the other hand, the Affidavit contains reliable information that [redacted]

[redacted]—all of which justify a finding of probable cause.

Further, the defendant mistakenly asserts that the warrant in *Bosyk* alleged that a user "viewed" a hyperlink with numerous child pornography images and then "clicked on that hyperlink to download child pornography." Dkt. No 82 at 10, 12. All that warrant alleged was that Bosyk's IP address was used to access a page on a file-sharing site containing encrypted child pornography files, and that a link to that page had been posted on a Tor site with images of child pornography and a password to download the files. *Bosyk*, 933 F.3d at 323. Unlike here, there was no allegation in *Bosyk* that the user was on Tor before his IP address accessed the site containing password-protected child pornography, nor was there an allegation that the user had actually viewed child sexual abuse material prior to or after accessing the site. Regardless, the Fourth Circuit reasoned, the contents of the affidavit established that it was likely the user saw the link on Tor, meaning that he likely knew it would take him to child pornography and that there was probable cause to search Bosyk's home for evidence of the user's access of the site with the intent to view child pornography. *Id.* at 325–26. Those same inferences can and should be drawn here. And while the defendant here complains that the Affidavit does not state [redacted], the Fourth Circuit explained in *Bosyk* that a warrant need only set forth facts to show a fair probability that a crime occurred and that the more incriminating version of events is likelier than any innocent alternative to establish probable cause. *Id.* at 328. Given the explanation of the many steps a user would need to take to find and access child sexual abuse material on the Target Website, the Affidavit meets that standard here.

Additionally, in a notice of supplemental authority, the defendant cites the unpublished 2017 district court decision in *Reece*, which he failed to include in his initial motion. Dkt. No. 93.

In *Bosyk*, 933 F.3d at 329, however, the Fourth Circuit rejected *Reece*, which involved a similar investigation, explaining that the *Reece* court erred by applying a heightened probable cause standard. At the hearing on the motion to suppress in the district court in *Bosyk*, Judge Leonie M. Brinkema also rejected *Reece* and found it so clear that the visit to the link provided "enough for probable cause to believe that there would be a computer in that residence that would have child pornography on it" that she did not reach the issue of good faith and did not permit defense counsel to present argument on the defendant's motion. *See* Exh. 2, Tr. of Mot. Hr'g, at 2–4.

Finally, assuming *arguendo* that the defendant's recurring suggestion that [redacted], courts have made clear that establishing probable cause for an access-with-intent offense under § 2252(a)(4)(B) "does not require a showing that [a defendant] actually viewed illegal content" on a site. *See United States v. Tagg*, 886 F.3d 579, 587–8 (6th Cir. 2018) ("[P]robable cause to search [defendant's] house would exist even if he was 'curiosity shopping' for child porn on [a Tor hidden service] but never actually viewed an illegal image."). Accordingly, the defendant's interpretation of the tip—which is contradicted by a plain and commonsense reading of the Affidavit and the tip itself—would have no effect on the probable cause determination

3. The information in the Affidavit was not stale

Third, the defendant asserts, without any support, that the 8.5 months between that date [redacted]—and the date the warrant issued—February 10, 2020—rendered it stale. Dkt. No. 82 at 13. But courts do not just count "the number of days between the occurrence of the facts supplied and the issuance of the affidavit" when evaluating staleness; rather, they look at "all the facts and circumstances of the

case, including the nature of the unlawful activity alleged, the length of the activity, and the nature of the property to be seized." *Richardson*, 607 F.3d at 370. In child pornography cases, courts "have sustained warrants issued many months, and even years, after the events that gave rise to probable cause." *Bosyk*, 933 F.3d at 331; *see also United States v. Davis*, 313 F. App'x 672, 674 (4th Cir. 2009) ("[I]nformation a year old is not stale a matter of law in child pornography cases."). This is because these offenders often hold on to such material, store it in secure places in their homes, and view it as digital files that can be forensically recovered even after being deleted. *Bosyk*, 933 F.3d at 330. Here, the Affidavit provided reason to believe that someone in the defendant's home intentionally sought out and accessed child pornography on Tor, that this individual had an interest in viewing child pornography, and that evidence of such activity would therefore likely still be recoverable from electronic devices in the home in February 2020. Accordingly, the defendant's staleness argument is without merit.

II. The Defendant's Remaining Motions to Suppress Should Also Be Denied

In his next three motions, the defendant argues that he is entitled to a *Franks* hearing to challenge the veracity of the Affidavit based on various complaints and allegations of omissions he raises throughout approximately 76 pages of briefing. Dkt. Nos. 84, 86, and 91. At base, however, his motions attack three parts of the Affidavit: (1) Paragraph 23, [redacted], Dkt. No. 86; (2) Paragraph 25, [redacted], Dkt. No. 91; and (3) miscellany paragraphs describing Tor, the Target Website, the internet, child pornography, and his home, Dkt. No. 84.

While a defendant "is generally not entitled to challenge the veracity of a facially valid" affidavit, the Supreme Court has "carved out a narrow exception to this rule, whereby an accused is entitled to an evidentiary hearing[.]" *United States v. Allen*, 631 F.3d 164, 171 (4th Cir. 2011) (citing *Franks v. Delaware*, 438 U.S. 154, 155–56 (1978)). To obtain such a hearing, the defendant must first make a "substantial preliminary showing" that (1) the affiant made a false statement, (2) the affiant did so "knowingly and intentionally, or with reckless disregard for the truth," and (3) that the statement was "necessary to the finding of probable cause." *United States v. White*, 850 F.3d 667, 673 (4th Cir. 2017) (quoting *Franks*, 438 U.S. at 155–56). In order to make the "rigorous" showing necessary for a *Franks* hearing, the defendant must provide more than conclusory assertions or a desire to cross-examine the affiant; he "should include affidavits or other evidence to overcome the presumption of the warrant's validity." *Clenney*, 631 F.3d at 663.

Importantly, when a defendant claims that an affidavit is misleading based on omissions, as the defendant does repeatedly throughout his motions, he faces an even higher burden. He must show that omissions were "*designed to mislead*, or . . . [were] made *in reckless disregard of whether they would mislead*." *United States v. Clenney*, 631 F.3d 658, 664 (4th Cir. 2011) (emphasis in original) (quoting *United States v. Colkley*, 899 F.2d 297, 301 (4th Cir. 1990)). He also must show that including the omissions in the affidavit "would defeat probable cause." *Id.* This heightened burden exists because, as another member of this Court warned, "invalidating warrants for omissions potentially opens officers to endless conjecture about the investigative leads, fragments of information, or other matters that might, if included, have redounded to the defendant's benefit," leading to "endless rounds of *Franks* hearings to contest facially sufficient warrants." *United States v. Young*, 260 F. Supp. 3d 530, 555 (E.D. Va. 2017) (citing *Colkley*, 899 F.2d at 301). Applying these principles, the defendant has failed to sustain his burden to obtain a

Franks hearing.

A. The Affidavit Does Not Contain Any Material and Knowingly or Recklessly False Statements or Omissions Regarding [redacted]

The defendant's motion regarding paragraph 23 of the Affidavit covers familiar ground. Dkt. No. 86. Repurposing the failed argument from his motion to compel, the defendant claims that [redacted], that SA Ford knew it was a lie, and that, presumably, SA Ford's decision not to add language to the Affidavit explaining that the tip was a lie consistent with the defendant's view of it was an intentional and material omission. *Id.* at 22–26. The primary basis for this theory is that at other times and in other places, SA Ford wrote only that [redacted] Based only on this minor distinction, the defendant speculates that the tip actually means that [redacted]. And, confusingly, the defendant now cites SA Ford's description of the tip in the same Affidavit as paragraph 23 as somehow simultaneously proving that he understood the tip to mean what the defendant claims it means, contrary to a commonsense reading of the tip, and that he also intentionally omitted this very information from the Affidavit in order to mislead the magistrate judge on this issue.

As the Court already explained, however, paragraph 23 is an accurate recitation of the tip, and a description of the tip as stating that [redacted] in no way contradicts the tip. Dkt. No. 73 at 9–11. The defendant also points to the brevity of the tip, the grammar in the

[redacted],[5] differences in fonts in the documents, and the possibility of [redacted]. The United States fails to see how these factors would have any impact on the reliability of the tip or SA Ford's understanding of its meaning. After all, it is entirely possible—and in fact likely—[redacted]. Moreover, the Affidavit specifically noted that [redacted]. Aff. at ¶ 26.

The defendant has also not identified anywhere in the Affidavit where SA Ford intentionally attempted to mislead the magistrate judge about the extent of the tip by claiming, for example, that [redacted]. In fact, the defendant has not pointed to a single instance in which SA Ford actually mischaracterized, exaggerated, or omitted information about the tip that is supported by anything other than the above wishful speculation. This is because the instant motion, while styled as a request for a *Franks* hearing, is really another attack on probable cause; the defendant does not believe the Affidavit based on this tip established probable cause to search his home and appears to think that no one—including the affiant and the magistrate judge—could have arrived at the contrary conclusion in good faith. In other words, his theory that the Affidavit contained intentional and material

[5] The defendant asserts that the term [redacted]. Dkt. No. 86 at 22. But that is simply not the case. Indeed, considering that this same document uses the [redacted]

omissions regarding the information in paragraph 23 is pure conjecture, and his motion for a *Franks* hearing should be denied.

1. Even if the defendant's theory about [redacted] is correct, he cannot show that the Affidavit misleadingly omitted material information

Even assuming *arguendo* that the defendant's theory about the meaning of the tip has some basis in fact—that is, that [redacted]—the defendant has failed to satisfy his burden of proving that the omission of this information was both designed to mislead and necessary to the probable cause determination as required to obtain a *Franks* hearing. In fact, as he points out in his motion, the Affidavit actually states that there was [redacted] and the magistrate judge still issued the warrant. Dkt. No. 86 at 24. This is because, as the Affidavit also noted, [redacted] did so knowingly and with the intent to view child pornography in violation of the law. Aff. at ¶ 30.

As explained above, courts have routinely held that an internet user accessing and viewing content on a hidden service dedicated to the sharing of child pornography provides probable cause to believe that the user was accessing or attempting to access the site with the intent to view child pornography. *See supra* p. 10 n.4. And, even going a step further and assuming that the defendant is somehow correct that [redacted], the inclusion of that information in the Affidavit would not defeat a finding of probable cause either. In the absence of evidence of membership to or downloads from a child pornography site, courts have looked to other factors about the site,

including the explicit nature of its title and welcome page, in determining whether accessing the site provides probable cause to search a home. *See United States v. Martin*, 426 F.3d 68, 75–76 (2d Cir. 2005) (finding that the welcome message of an online child pornography trading group titled "girls12–16" made plain "its essential purpose to trade child pornography"). Here, [redacted]. Aff. at ¶¶ 17, 19. Accordingly, even if the defendant's unsupported theory about what [redacted] meant is correct, and even if his speculation that SA Ford shared his view of the meaning of the tip is true, he cannot show that including this information would defeat probable cause. Accordingly, his motion for a *Franks* hearing should be denied.

B. The Affidavit Does Not Contain Any Material and Knowingly or Recklessly False Statements or Omissions Regarding [redacted]

The defendant's next motion to suppress, which focuses on paragraph 25 of the Affidavit, also covers familiar ground. Dkt. No. 91. In it, he seeks to re-litigate the theory from his motion to compel that: [redacted] that SA Ford knew this; and that, presumably, SA Ford's decision not to tack on language to the description of the tip in the Affidavit that conforms with the defendant's theory constitutes a knowing and material omission that misled the magistrate judge. *Id.* at 12–16. To support his theory, the defendant provides declarations from three purported experts, none of whom know what [redacted]. Contrary to the defendant's claims, however, none of his purported experts have asserted that [redacted]

[redacted], meaning he has failed to make a substantial preliminary showing that the Affidavit contained a knowing and material omission with respect to this topic. [redacted]. But, as he appears to concede, he has no evidence to support this theory beyond his own speculation. Accordingly, and for the reasons below, this motion should be denied as well.

1. The Affidavit accurately describes [redacted] and the defendant cannot make a substantial preliminary showing that the tip is false

As the Court explained in its prior opinion rejecting this argument, paragraph 25 accurately describes the tip and the defendant has provided no basis for questioning the veracity of this portion of the Affidavit. Dkt. No. 73 at 12. In his instant motion, however, the defendant doubles down on his theory that the FBI knew that [redacted]. Indeed, in the declarations by Matthew Ryder, [redacted]. Dkt. No. 91, Exhs. 7 & 8. Similarly, in what is now his fourth declaration, Dr. Matthew Miller, an associate professor of computer science, only opines again that he believes [redacted]

[6] The defendant's current theory is that [redacted]

[redacted].

Dkt. No. 91, Exh. 6 at 4–5. In other words, for the fourth time, Dr. Miller has failed to comment on anything specific to [redacted] Dkt. No. 91 at 13.

The defendant has also submitted a declaration by Dr. Richard Clayton, identified as the Director of the Cambridge Cybercrime Centre at the University of Cambridge. Dkt. No. 91, Exh. 9. In his declaration, [redacted].[7] *Id.* at 8. And while Dr. Clayton opines that [redacted]. *Id.*

[redacted]

[7] [redacted]

[redacted]. Dkt. No. 91 at 12–13. But, as the Court has already explained, [redacted] Dkt. No. 73 at 12. [redacted].

The defendant also attacks SA Ford's August 10, 2020, declaration regarding [redacted] that was provided during the briefing on the defendant's motion to compel. Specifically, the defendant claims that it proves that SA Ford [redacted] Dkt. No. 91 at 15–16. This claim, however, is based on selective quotes that misrepresent the declaration, which only describes the steps SA Ford took to prepare the declaration and does not address his prior knowledge. More importantly, the defendant's continued assertion that [redacted]

Finally, in a last ditch attempt to establish that paragraph 25 is intentionally and materially misleading, the defendant floats the idea [redacted]. Dkt. No. 91 at 16–17. Setting aside the fact that [redacted]

[redacted] the defendant's latest theory is based on pure speculation and a misreading of Dr. Clayton's declaration. Indeed, Dr. Clayton [redacted] Dkt. No. 91, Exh. 9 at 9–10. This sort of hypothesizing cannot sustain the heavy burden required for a *Franks* hearing.

2. Even if the defendant's theory about [redacted] is correct, he cannot show that the Affidavit misleadingly omitted material information

The defendant's claim that the FBI [redacted], Dkt. No. 91 at 13, has no basis in fact. But even if the defendant's theory is partially true and [redacted], he has failed to show how the omission of that possibility was intentionally and materially misleading. As described above, both SA Ford and the defendant's own purported expert, Dr. Clayton, have noted that [redacted] The suggestion that SA Ford was required to engage in the same rank speculation that the defendant is engaging in now and then include that speculation in the Affidavit has no support in the law and would not undermine all the other indicia of [redacted] included in the Affidavit. Accordingly, the defendant's motion should be denied.

3. The defendant's claim that the United States and [redacted] is baseless

The defendant also argues that, had the Court granted his motion to compel, he would have found support for his baseless theory that the FBI was [redacted]. Dkt. No. 91

at 17–20. As the defendant acknowledges, however, he has no evidence to support this claim, *id.* at 18, and both [redacted] and the statements in the Affidavit affirmatively reject this theory. Aff. at ¶ 25. In short, as the Court explained before, the defendant's suggestion that the FBI [redacted] Dkt. No. 73 at 13. Additionally, the defendant's claim that he [redacted].

C. The Affidavit Does Not Contain Any Material and Knowingly or Recklessly False Statements or Omissions in Any of the Other Sections Identified by the Defendant

The defendant dedicates his final motion, which is almost 30 pages long, to providing a litany of complaints about various parts of the Affidavit that he claims omit material information—including information about Tor, the Target Website, the intent of the user of the Target IP, where forensic evidence could be recovered, and his mother—and then asserts that he is entitled to a *Franks* hearing. Dkt. No. 84. This motion, which focuses on omissions from the Affidavit as opposed to false statements that were affirmatively included, is exactly the type of *Franks* motion that the Fourth Circuit cautioned would lead to "endless conjecture" about "fragments of information" that may have "redounded to the defendant's benefit" without being dispositive. *Colkley*, 899 F.2d at 301. In any event, none of the alleged omissions the defendant identifies

would defeat probable cause if included, and he has not made any showing, let alone a substantial one, that SA Ford intentionally omitted the information he believes should have been included to mislead the magistrate judge. Accordingly, this motion should be denied.

As an initial matter, several of the omissions the defendant identifies are far-fetched and obviously not dispositive. For example, he inexplicably claims that omitting that his mother is a psychologist was material because she may have visited the Target Website for work, as if those circumstances make the knowing access of a child pornography site legal. Dkt. No. 84 at 23. He also suggests that the neutral description of how Tor seeks to provide anonymity creates a patina of suspicion, and argues that including that the United States was involved with creating Tor would somehow better explain those anonymity features. *Id.* at 17. In yet another section of his motion, he asserts that the Affidavit misleadingly described the Target Website as dedicated to the distribution and advertisement of child pornography, but the only basis he appears to have for his claim is that, in another part of the Affidavit, SA Ford [redacted] *Id.* at 18. And in still other portions of his motion, the defendant complains that SA Ford did not more strenuously note the absence of certain facts, such as the lack of any allegation that the Target IP was used to register an account with the site. *Id.* at 18. As the Fourth Circuit explained in *Bosyk*, 933 F.3d at 332, however, "agents need not include disclaimers specifically pointing out facts absent from the affidavit to obtain a warrant" because a "warrant application is 'judged on the adequacy of what it does contain, not on what it lacks, or on what a critic might say should have been added.'" (quoting *United States v. Allen*, 211 F.3d 970, 975 (6th Cir. 2000)). And here, the Affidavit accurately explained the information known to the FBI and provided the magistrate judge with a fair opportunity to assess the strength of the government's evidence.

Setting these alleged omissions aside, the remainder of the defendant's motion relies on misrepresenting the Affidavit in an effort to undermine the reasonable inferences that judges across the country have drawn to find probable cause to search a home based on [redacted].[8] *See supra* p. 10 n.4. The defendant relies heavily on declarations by Seth Schoen[9] and Dr. Matthew Miller to argue that the Affidavit misleadingly states that there are no search engines on Tor, but the Affidavit does not state that. Rather, it states that "[h]idden service websites on the Tor Network are not 'indexed' by search engines like Google *to anywhere near the same degree as websites that operate on the open Internet*." Aff. at ¶ 27 (emphasis added). Neither declaration cited by the defendant disputes that fact. More importantly, neither declaration provides any information about whether the Target Website specifically was discoverable through a Google-type search on Tor in May 2019 and, if so, what the likelihood was of finding the site that way using innocent search terms.[10] Absent such evidence, the defendant cannot establish that these alleged omissions are material because, as the Fourth Circuit has explained, an affidavit need not rule out every innocent explanation to establish probable cause. *Bosyk*, 933 F.3d at 327. Instead, it simply needs to provide a fair probability to believe that an incriminating version of events occurred. *Id.* And as the Fourth Circuit further explained in *Bosyk*, courts should be particularly skeptical of possible innocent explanations for accessing hidden

[8] For example, the defendant incorrectly describes paragraph 27 of the Affidavit as stating that the only way to access the Target Website is through a directory site or by typing—as opposed to finding, which is what the Affidavit states—the site's unique web address. Dkt. No. 84 at 19.

[9] Seth Schoen is identified as a computer technologist who previously worked for a non-profit organization focused on advocating for individuals' internet privacy rights. Dkt. No. 84, Exh 7.

[10] Dr. Miller opines that the user of the Target IP "likely could have navigated to the TARGET website by clicking on a search engine result or by clicking on a link, as opposed to typing the 16-or-56-character web address," but he provides no basis for his opinion other than the fact that search engines exist on Tor. Dkt. No. 84, Exh. 6 at 7.

services dedicated to child pornography given that online pedophiles "often take steps to conceal their contraband material" and "frequently employ complex measures to keep their online activities secret." *Id.*

The defendant also claims that the Affidavit was misleading by suggesting that there was reason to believe someone in his home had an interest in viewing sexually explicit visual depictions of children. His claim is based on: (1) the speculation that the Target Website may have been accessible through a Google-type search on Tor; [redacted] More generally, the defendant's suggestion that a single instance of accessing online child sexual abuse material on a secretive Tor hidden service dedicated to sharing child pornography is insufficient to support the inference that someone in the defendant's home had an interest viewing child pornography has been rejected by courts in factually similar circumstances. *See*, *e.g.*, *Bosyk*, 933 F.3d at 331–32 ("We think it is possible to infer from the affidavit that whoever clicked on the link did so willfully and deliberately because he was interested in images of child pornography."). Relatedly, his claim that the Affidavit misled the magistrate judge about the possibility of finding forensic evidence on electronic devices ignores the well-supported and frequently drawn inference that individuals who have an interest in viewing child pornography often retain such content for years on computers or as digital files. Aff. at ¶¶ 37–46.

At the very best, all the defendant has done in his final motion is identify disclaimers and information that might have been "potentially relevant" but were in no way dispositive of probable cause, and then offer a conclusory accusation that this information was omitted intentionally to mislead the magistrate judge. Based on this, the defendant has failed to make the requisite showing for a *Franks* hearing, and the motion should be denied.

III. The Good Faith Exception, If Necessary, Defeats the Motions to Suppress

For the same reasons discussed above, the good-faith exception under *United States v. Leon*, 468 U.S. 897 (1984), applies such that suppression is not the appropriate remedy. Not every Fourth Amendment violation justifies suppression of evidence. *Herring v. United States*, 55 U.S. 135, 140 (2009). In fact, it is a remedy of "last resort." *Hudson v. Michigan*, 547 U.S. 586, 591 (2006). Suppression is appropriate when, and only when, its "substantial social costs" are outweighed by the benefits of deterring "deliberate," "reckless," or "grossly negligent" misconduct. *Davis v. United States*, 564 U.S. 229, 236–37 (2011). Where law enforcement acts with "objective good faith" that their conduct was legal, however, suppression is not appropriate. *Leon*, 468 U.S. at 920.

The good-faith exception is inapplicable in only four circumstances: (1) "if the magistrate . . . was misled by information in an affidavit that the affiant knew was false"; (2) if the magistrate judge "wholly abandoned his judicial role"; (3) if the affidavit is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; and (4) if the warrant is so facially deficient "that the executing officers cannot reasonably presume it to be valid." *United States v. Doyle*, 650 F.3d 460, 467 (4th Cir. 2011). The defendant appears to elliptically make reference to all four exceptions across his four motions, though he provides no elaboration. Dkt. Nos. 82 at 14, 84 at 25, 86 at 29, & 91 at 20–21. As explained above, however, the Affidavit in

this matter was entirely truthful, contained no information intentionally designed to mislead the magistrate judge, and contained enough information to meet the probable cause threshold as evidenced by Magistrate Judge Anderson's issuance of the warrant. *Leon*, 468 U.S. at 922, 925 (explaining that a magistrate judge's issuance of a warrant is typically enough to establish good faith reliance on it). In these circumstances, the law is clear: to the extent there are any deficiencies in the Affidavit, the good faith exception applies and the defendant's four motions to suppress should be denied.

CONCLUSION

For the foregoing reasons, the government respectfully requests that the Court deny the defendant's motions to suppress.

Respectfully submitted,

G. Zachary Terwilliger
United States Attorney

Date: September 9, 2020 By: /s/

William G. Clayman
Special Assistant United States Attorney (LT)
Jay V. Prabhu
Assistant United States Attorney
United States Attorney's Office
2100 Jamieson Avenue
Alexandria, Virginia 22314
Phone: 703-299-3700
Fax: 703-299-3981
Email: William.G.Clayman@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on September 9, 2020, I emailed an un-redacted copy of the foregoing to all counsel of record and will filed the foregoing with the Clerk of Court.

By: /s/

William G. Clayman
Special Assistant United States Attorney (LT)
United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, Virginia 22314
(703) 299-3700
Email: william.g.clayman@usdoj.gov